IN THE CLAIMS:

1. (Currently Amended) A computer program product for automatically determining if a packet is a new, exploit candidate, said program product comprising:

a computer readable medium;

first program instructions to determine if said packet is a known exploit or portion thereof;

second program instructions to determine if said packet is addressed to a broadcast IP address of a network;~~network broadcast traffic presumed to be harmless;~~ and

third program instructions to determine if said packet is network administration traffic; ~~wherein~~

fourth program instructions, responsive to said packet being a ~~if said packet is said~~ known exploit or portion thereof, addressed to a broadcast IP address of a network, ~~broadcast traffic,~~ or network administration traffic, to determine that said packet is not ~~considered~~ a new, exploit candidate; and

fifth program instructions, responsive to said packet not being a ~~if said packet is not said~~ known exploit or portion thereof, addressed to a broadcast IP address of a network, ~~broadcast traffic, or~~ network administration traffic or another type of traffic known to be benign, to determine and report that ~~,~~ said packet is a new, ~~an~~ exploit candidate; and wherein

said first, second, ~~and~~ third, fourth and fifth program instructions are embodied~~recorded~~ on said medium.

2. (Currently Amended) A computer program product as set forth in claim 1 further comprising:

sixth~~fourth~~ program instructions to determine if said packet is web crawler traffic; and wherein

said fourth program instructions are responsive to ~~if~~ said packet being a~~is said~~ known exploit or portion thereof, addressed to a broadcast IP address of a network, ~~broadcast traffic,~~ network administration traffic or web crawler traffic, to determine that said packet is not ~~considered~~ a new, exploit candidate; and

said fifth program instructions are responsive to ~~if~~ said packet ~~is~~ not being a ~~said~~ known exploit or portion thereof, addressed to a broadcast IP address of a network, ~~broadcast traffic,~~ network administration traffic or web crawler traffic, to determine that said packet is a new, ~~an~~ exploit candidate; and

said sixth~~fourth~~ program instructions are embodied~~recorded~~ on said medium.

3. (Original) A computer program product as set forth in claim 1 wherein said first program instructions determine if said packet is a known exploit or portion thereof by searching said packet for a known signature of said known exploit.

4. (Original) A computer program product as set forth in claim 1 wherein said first program instructions determine if said packet is a known exploit by comparing an identity of said packet to one or more identities, sent by an intrusion detection system, of respective packet(s) which said intrusion detection system determined to contain a known exploit or portion thereof.

5. (Original) A computer program product as set forth in claim 1 wherein said packet was received by a computing device at an unused IP address, and said program product is executed at said computing device.

6. (Currently Amended) A computer program product as set forth in claim 1 further comprising: ~~5 wherein said computing device is a honeypot.~~

sixth program instructions, responsive to said fifth program instructions determining that said packet is a new exploit candidate, to determine a signature of said packet or a sequence of packets including the first said packet, and report said new exploit candidate and said signature to an administrator; and wherein

said sixth program instructions are embodied on said medium.

7. (Currently Amended) A computer program product as set forth in claim 6 wherein if said fourth program instructions determine that said packet is not a new, exploit candidate, then a signature of said packet or a sequence of packets including said first packet is not determined. ~~+ further comprising:~~

~~fourth program instructions to determine if said packet is broadcast traffic, and wherein~~

~~if said packet is said known exploit or portion thereof, broadcast traffic, or network administration traffic, said packet is not considered a new, exploit candidate; and~~

~~if said packet is not said known exploit or portion thereof, broadcast traffic, or network administration traffic, said packet is an exploit candidate; and~~

~~said fourth program instructions are recorded on said medium.~~

8. (Currently Amended) A computer program product as set forth in claim 1~~7~~ wherein said second~~fourth~~ program instructions determines if said packet is addressed to a broadcast IP address of said network ~~broadcast traffic based on a gateway IP address and netmask of said packet.~~ by comparing a destination IP address of said packet to a gateway IP address and netmask of said network which identifies a broadcast IP address of said network.

9. (Currently Amended) A computer program product as set forth in claim 1 wherein:

said second program instructions also determines if said packet has ~~is said network broadcast traffic by comparing~~ a protocol listed in ~~of said packet to~~ a list of protocols assumed to be harmless network broadcast traffic

said fourth program instructions is responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or having a protocol listed in a list of protocols assumed to be harmless network broadcast traffic, to determine that said packet is not a new, exploit candidate; and

said fifth program instructions is responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network or network administration traffic and not having a protocol listed in a list of protocols assumed to be harmless network broadcast traffic, to determine and report that said packet is a new, exploit candidate.

10. (Currently Amended) A computer program product as set forth in claim 1 wherein said third program instructions determines if said packet is network administration traffic by comparing an IP protocol and IP address of said packet to a list of combinations of IP protocols and IP addresses assumed to be network administration traffic.

11. (Currently Amended) A computer program product as set forth in claim 2 wherein said sixth~~forth~~ program instructions determines if said packet is web crawler traffic by comparing an IP address of said packet to a list of IP addresses of known web crawlers.

12. (Currently Amended) A computer program product as set forth in claim 1 further comprising sixth program instructions, responsive to ~~wherein if~~ said packet ~~is~~ not being ~~said~~ a known exploit, network broadcast traffic, ~~or~~ addressed to a broadcast IP address of a network ~~administration traffic~~ or other type of traffic known to be benign, ~~further comprising: fourth program instructions~~ to identify a sequence of packets including the first said packet, said sequence of packets being a new, exploit candidate; and wherein

said sixth~~forth~~ program instructions are embodied~~recorded~~ on said medium.

13. (Currently Amended) A computer system for automatically determining if a packet is a new, exploit candidate, said system comprising:

means for determining if said packet is a known exploit or portion thereof;

means for determining if said packet is addressed to a broadcast IP address of a network; ~~broadcast traffic presumed to be harmless;~~ and

means for determining if said packet is network administration traffic; wherein

means, responsive to ~~if~~ said packet being~~is~~ said known exploit or portion thereof, addressed to said broadcast IP address of said network, ~~broadcast traffic,~~ or network administration traffic, for determining that said packet is not ~~considered~~ a new, exploit candidate; and

means, responsive to~~if~~ said packet ~~is~~ not being a~~said~~ known exploit or portion thereof, addressed to said broadcast IP address of said network, ~~broadcast traffic, or~~ network administration traffic or another type of traffic known to be benign, for determining and reporting that, said packet is a new,~~an~~ exploit candidate.

14. (Currently Amended) A computer system as set forth in claim 13 further comprising:

means for determining if said packet is web crawler traffic; and wherein

said means for determining that said packet is not a new, exploit candidate determines that said packet is not a new exploit candidate if said packet is ~~said known exploit or portion thereof, network broadcast traffic, network administration traffic or~~ web crawler traffic, ~~said packet is not considered a new, exploit candidate; and~~

~~if said packet is not said known exploit or portion thereof, network broadcast traffic, network administration traffic or web crawler traffic, said packet is an exploit candidate.~~

15. (Currently Amended) A computer system as set forth in claim 13 wherein said packet was received by said computer system in said network at an unused IP address.

16. (Currently Amended) A computer system as set forth in claim 13 further comprising means, responsive to said packet not being a new exploit candidate, for determining a signature of said packet or a sequence of packets including the first said packet, and reporting said new, exploit candidate and said signature to an administrator, ~~wherein said computer system is a honeypot.~~

Claims 17-20 (Canceled)

Please enter new claims 21-24, as follows:

21. (New) A computer program product for automatically determining if a packet is a new, exploit candidate, said program product comprising:

a computer readable medium;

first program instructions to determine if said packet is a known exploit or portion thereof;

second program instructions to determine if said packet is addressed to a broadcast IP address of a network;

third program instructions to determine if said packet has a protocol listed in a list of protocols assumed to be harmless broadcast traffic;

fourth program instructions to determine if said packet is network administration traffic;

fifth program instructions, responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network or network administration traffic or having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine that said packet is not a new, exploit candidate; and

sixth program instructions, responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network or network administration traffic and not having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine and report that said packet is a new, exploit candidate; and wherein

said first, second, third, fourth, fifth and sixth program instructions are embodied on said medium.

22. (New) A computer program product as set forth in claim 21 further comprising:

seventh program instructions to determine if said packet is web crawler traffic; and wherein

said fifth program instructions are responsive to said packet being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic or having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine that said packet is not a new, exploit candidate; and

said sixth program instructions are responsive to said packet not being a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or web crawler traffic or other traffic known to be benign or having a protocol listed in a list of protocols assumed to be harmless broadcast traffic, to determine that said packet is a new, exploit candidate; and

said seventh program instructions are embodied on said medium.

23. (New) A computer program product as set forth in claim 21 further comprising:

seventh program instructions, responsive to said sixth program instructions determining that said packet is a new, exploit candidate, to determine a signature of said packet or a sequence of packets including the first said packet, and report said new, exploit candidate and said signature to an administrator; and wherein

said seventh program instructions are embodied on said medium.

24. (New) A computer program product as set forth in claim 21 wherein said second program instructions determine if said packet is addressed to a broadcast IP address of said network by comparing a destination IP address of said packet to a gateway IP address and netmask of said network which identifies a broadcast IP address of said network.